# Electronic Information Management (EIM)

## Business Rules and Practices

Discussion Draft
June 2004

Alberta
GOVERNMENT OF ALBERTA

*Produced by:*

Information Management Branch
Government and Program Support Services
Alberta Government Services
3rd Floor, Commerce Place
10155 – 102 Street
Edmonton, Alberta, Canada
T5J 4L4

Office Phone: (780) 422-2657
Fax: (780) 427-1120

Web sites:
www.im.gov.ab.ca
www.gov.ab.ca/foip
www.pipa.gov.ab.ca

**© Government of Alberta**

**ISBN 0-7785-3126-0**

105-00666/



# Contents

**Foreword** ..... 1
*Objective* ..... 1
*Electronic Information Management (EIM)* ..... 1
*Organization of Business Rules and Practices* ..... 1

**1. Creation, Collection and Receipt** ..... 3
*1.1 Official Records Managed with EIM* ..... 3
*1.2 Other records to be managed within EIM* ..... 3
*1.3 Draft Documents* ..... 4
*1.4 Ministry Publications* ..... 4
*1.5 Profiling Documents in EIM – Metadata* ..... 4
*1.6 Profiling Collections of Content Items* ..... 5
*1.7 Profiling Databases and Applications* ..... 5
*1.8 Versions of Documents* ..... 5
*1.9 Electronic Mail Messages and Attachments* ..... 6
*1.10 Declaring Official Records* ..... 7
*1.11 Collaborative Document Authoring* ..... 7
*1.12 Date Functions* ..... 8
*1.13 Naming Electronic Documents* ..... 8
*1.14 Dynamic Links* ..... 8
*1.15 Quality Control* ..... 8

**2. Organization, Transmission, Use and Retrieval** ..... 9
*2.1 Records Classification Structure – Ministry* ..... 9
*2.2 Records Classification Structure – Program or Workgroup* ..... 9
*2.3 Folder Metadata* ..... 9
*2.4 User Profile* ..... 10
*2.5 Maintaining Audit Data* ..... 10
*2.6 Information Access* ..... 10
*2.7 Search and Retrievals* ..... 11
*2.8 Modifying Draft Content Items* ..... 11
*2.9 Deleting Content Items* ..... 11
*2.10 Remote Access to EIM* ..... 11
*2.11 Quality Control – Organization, Transmission, Use and Retrieval* ..... 12

**3. Storage and Protection** ..... 13
*3.1 Storage of Electronic Content Items and Profiles* ..... 13
*3.2 Storage of Metadata* ..... 14
*3.3 Inherit Security Attributes of Records Classification Code* ..... 14
*3.4 Access Restrictions* ..... 14
*3.5 Rights and Privileges* ..... 15
*3.6 Inherit Vital Records Attributes of Records Classification Code* ..... 15
*3.7 Vital Records – Disaster Recovery* ..... 16
*3.8 Migrating Content Items to Upgraded Software* ..... 16
*3.9 Transferring Access Rights to a Different User* ..... 16
*3.10 Transferring Content Items to a Different Workgroup* ..... 17
*3.11 Quality Control: Storage and Protection* ..... 17

**4. Retention and Disposition.....18**
*4.1 Retention – Assigning Retention Periods.....18*
*4.2 Inherit Retention Period Assigned to Records Classification Code.....18*
*4.3 Retention Period – Extend or Suspend.....19*
*4.4 Disposition – Records Retention and Disposition Schedule.....19*
*4.5 Disposition – Metadata.....19*
*4.6 Disposition – Folder Metadata.....19*
*4.7 Disposition – Workgroup Manager Approval.....20*
*4.8 Retention and Disposition – Records Classification Structure Audit Trail.....20*
*4.9 Final Disposition.....20*
*4.10 Quality Control: Retention and Disposition.....21*

**Glossary.....22**

# Foreword

## *Objective*

The effective implementation of electronic information management (EIM) will require a set of business rules and practices that are common across the ministry. This document has been developed to assist ministries in the development of these practices. It includes corporate as well as suggested ministry practices related to the use of EIM. In cases where a corporate practice has not been established, ministries may want to adapt the suggested practice to meet their business needs. The intention is to reduce the time taken by ministries to develop common practices before "rolling-out" EIM.

These business rules and practices should be used in conjunction with other tools developed to assist ministries with the implementation of EIM. These tools include:

- Corporate Functional Requirements,
- Model Ministry Accountability Structure, and
- Implementation Planning Guidance.

## *Electronic Information Management (EIM)*

EIM introduces the required consistent and systematic approach to managing all information assets, regardless of the medium in which they are held, throughout their entire life cycle. The vision is to have an integrated repository of information assets (i.e., content), including an integrated approach to metadata management within the ministry that includes:

- the output from collaboration processes (e.g., instant messages, e-meetings, e-rooms);
- office documents (e.g., word processing, spreadsheets, presentations) in the development stage;
- declared official records (including e-mail messages);
- imaged or scanned records (e.g., records with official signatures or those that are received in paper form that the ministry needs to capture electronically);
- links to paper, microform and other non-electronic records held in paper repositories; and
- links to application systems data.

## *Organization of Business Rules and Practices*

These draft business rules and practices are organized into four categories that follow the information lifecycle of documents and records:

- Creation, Collection and Receipt.
- Organization, Transmission, Use and Retrieval.
- Storage and Protection.
- Retention and Disposition.

They were developed through workshops with ministry representatives in the Fall of 2003. As a whole, they have been validated in consultation with a small sample of business managers in the Government of Alberta.

EIM business rules and practices can be set at three levels:

- Corporate (consistent EIM practice across all of government)
- Ministry (consistent EIM practice across all of a particular ministry, but may vary from ministry to ministry)
- Program (consistent EIM practice across a particular program areas, but practice may vary within the ministry and between ministries.)

In the case of **corporate** (GoA), the practice may be set by policy, legislation or standard-setting procedures. In these cases, the lead has been identified. Proposed corporate practices appear in **bold** in the text.

For **ministry**-level, there is a suggested practice for each.

There are no examples of practices set **only** at the program level. However, there are cases (e.g., metadata) where program areas may want to implement practices in addition to corporate or ministry practices.

In Phase 2 of the EIM Project, these business rules and practices will be validated and adapted based on pilot projects within ministries.

# 1.
# Creation, Collection and Receipt

[Note: Throughout this document, practices that are established at the corporate level are in **bold** text.]

All employees are responsible for record keeping. This means documenting their activities by creating, collecting and receiving records related to their business so that recorded information will be available, understandable and usable. Record keeping should comply with documentation standards for scientific and professional practice where these standards have been formally adopted.

## *1.1 Official Records Managed with EIM*

**All official records are to be managed within EIM. Exclusion: Records of the Minister that are of a personal or constituency and political nature.**

**A record is a record of information in any form, and includes notes, images, audio visual recordings, x-rays, books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any manner, but does not include software or any mechanism that produces records.**

**Official records do not include transitory records. A transitory record is a record containing information of temporary value which does not have some future administrative, financial, legal, research, or historical value to the government. This would include such information as duplicate records, draft documents, working materials, publications, blank forms, and temporary notes that do not have long-term value. [Lead: Government Services, Information Management Branch]**

## *1.2 Other records to be managed within EIM*

The following types of records may also be managed within EIM.

- Records that are needed to conduct work and have not yet been declared an official record.
- Non-business information that is of a purely private nature (i.e., of the individual employee such as lists, photos, electronic mail messages).

A duplicate of an electronic or non-electronic item is normally considered a transitory record and can be destroyed at will in accordance with the transitory records schedule and the rules for the destruction of transitory records.

If changes, or notations, are made to a duplicate it becomes a new record and must be managed within EIM as an official record. It must then be retained and disposed of according to approved retention and disposition schedules.

For records created within EIM, the electronic form will be considered the record. Paper duplicates that are used for convenience will be considered transitory unless annotated in any substantive way.

Responsibility: Controller

### 1.3 *Draft Documents*

Drafts of electronic and non-electronic documents created in the conduct of official ministry business are considered to be records and should be managed within EIM. More than one individual can author a draft document.

A draft document that is never communicated beyond a single author of the document may be considered a transitory record and may be destroyed.

An annotated draft, where the additional information is found in subsequent versions, may be considered to be a transitory record and can be destroyed at will. (Exception: where the annotations serve as evidence of the evolution of a document; the document should be declared an official record and managed in EIM.)

Responsibility: Controller

### 1.4 *Ministry Publications*

The original of a publication, (e.g., reproduction proof or camera ready copy), including periodicals, in electronic or non-electronic form, produced by or for the ministry will be managed in EIM.

Responsibility: Controller/Steward

### 1.5 *Profiling Documents in EIM – Metadata*

**Documents managed within EIM must be profiled. Profiling will include the following mandatory metadata elements:**

- **title,**
- **agent,**
- **subject,**
- **description,**
- **date created**

- **dates modified,**
- **security classification,**
- **aggregation level,**
- **record identifier,**
- **location; and**
- **disposition.**

**Note**: This is a draft standard at this point. [Lead: Government Services, Information Management Branch]

The author, a delegate or the workgroup EIM Administrator can modify metadata values assigned to an electronic document.

[*Ministries may develop additional metadata requirements.*]

[*Program areas may develop program-specific metadata requirements.*]

Responsibility: Controller, with assistance from Administrator and Steward

### 1.6 *Profiling Collections of Content Items*

Special collections of content items, such as photographs, periodicals, reference material or videos, should be profiled within EIM. The profile will describe the subject of the collection, its location, the responsible organization and, if appropriate, a contact person.

Responsibility: Controller/Steward

### 1.7 *Profiling Databases and Applications*

Applications (e.g. databases and other collections of structured data) should be profiled within EIM. The profile will describe the subject of the collection, its location, the responsible organization and, if appropriate, a contact person.

Responsibility: Steward/Administrator

### 1.8 *Versions of Documents*

Versions of electronic and non-electronic documents are to be created, where necessary, and managed within EIM.

Versions of the following types of records should be maintained and declared official records:

- legislation;
- legal documents;

- policies, standards, guidelines and procedures;
- audit reports; and
- accounting working papers

Consideration should be given to creating versions of other types of records to facilitate work and document transactions, including:

- technical specifications;
- requests for proposals;
- action requests;
- briefing notes; and
- reports.

**Note**: There is no limit on the number of versions that can be created. Once a new version of an electronic document is created, any prior version cannot be modified, if they have been declared official records.

In some cases, versions may be used by authors as a means of managing work. The author can delete previous versions of an electronic document, if the record is transitory.

Responsibility: Controller

## 1.9 *Electronic Mail Messages and Attachments*

Electronic mail messages and attachments created or received in the course of conducting ministry business will be managed in EIM.

Exclusions:

- transitory e-mail records;
- attachments that are duplicate records;
- administrative messages, (e.g., booking a meeting room);
- information copies, (e.g., copy of a broadcast message having no operational value); and
- personal messages, (e.g., arrange a social meeting).

**Note**: Attachments that are maintained within the same repository as the body of the message (e.g. same ministry) do not need to be managed with the e-mail message as long as it is clear what attachment is referred to in the message and that attachment can be produced for evidentiary purposes. Attachments maintained in another repository (e.g., other ministry, outside organization), must be managed as part of the e-mail message if the e-mail message has been declared an official record.

**Note**: An electronic message which has been included in its entirety within the body of a subsequent electronic message that cites the same subject, as in a "Reply With History," can be deleted as a transitory record.

Responsibility: For electronic mail messages that are declared official records, the following responsibilities apply for managing and profiling these records:

- for electronic mail messages sent within a ministry, it is the responsibility of the author to manage the electronic mail messages in EIM; in the case of e-mail threads, it is the responsibility of the author of the original message of the thread;
- for electronic mail messages from outside the ministry, it is the responsibility of the recipient to manage the electronic message in EIM;
- electronic mail messages received from outside the ministry and addressed to multiple recipients within the ministry, are to be managed in EIM by the person in that workgroup who appears first on the list of recipients *[ministries may want to modify this practice, as needed.]*

### 1.10 Declaring Official Records

It is the responsibility of the document's author, a delegate or the workgroup EIM Administrator to declare a document as an official record to protect it from alteration and to assure its integrity.

When a document is declared a final record, the author identified in the document profile assumes accountability for its content.

Official record status may be assigned to drafts and versions of a document in progress—to show a document's evolution

Responsibility: Controller/Administrator

### 1.11 Collaborative Document Authoring

For documents authored collaboratively, i.e., by two or more people, one person will be assigned the responsibility for:

- managing the document within EIM;
- declaring them as official records when appropriate; and
- setting and removing access restrictions.

Co-authors will have full access and editing rights to the document, such as:

- creating new versions as appropriate; and
- deleting the document if declared a transitory record.

Responsibility: Controller

### 1.12 Date Functions

Date Functions (e.g., automatic dating feature in MS Office) should not be used in documents. If used in the document creation process, they should be replaced with the appropriate date in standard text format before the document can be profiled and stored in EIM.

Responsibility: Controller

### 1.13 Naming Electronic Documents

*[Ed. Note: Ministries will want to develop standard naming conventions for electronic documents. A sample practice is identified here, however corporate guidance is still being worked on.]*

All documents stored managed in EIM will use the following naming protocol

Subject_version_date.ext

The subject is the title of the document. The version is the version number. The date is the date the document is created or updated and should be in the international date standard. The extension identifies the program in which the document was created (e.g., Word, Excel, PowerPoint, etc.).

Responsibility: Controller

### 1.14 Dynamic Links

A document containing dynamic links to other documents can be managed in EIM but there is no guarantee that the linked documents will be the same upon each use, particularly if control of the linked documents rests with another workgroup or with someone outside the ministry.

It is the responsibility of the person who makes a decision, based on a document containing dynamic links, to manage a copy of the complete document set within EIM, as it existed at the time the decision was made.

Responsibility: Controller/User

### 1.15 Quality Control

The workgroup EIM Administrator will be responsible for performing quality control on all aspects associated with the creation, collection and receipt of records managed within EIM. This will include monitoring the workgroup's use of EIM to identify problems relating to filing official records created, collected or received by the workgroup.

Responsibility: Administrator

# 2.
# Organization, Transmission, Use and Retrieval

Records will be identified, described and organized according to approved records classification structures that support decision-making and program delivery. Corporate inventories of records holdings will be maintained to support access and retrieval. A records classification structure and related procedures will be maintained for retrieving, describing, and organizing records holdings.

## *2.1 Records Classification Structure – Ministry*

A records classification structure will be maintained at the ministry level to link all ministry programs, projects and information holdings. The ministry records classification structure will be based on relevant government policies and guidelines.

Responsibility: Senior Records Officer

## *2.2 Records Classification Structure – Program or Workgroup*

A records classification structure for organizing, describing and facilitating the management of records in all media will be maintained within all workgroups. The workgroup records classification structure will be managed at the ministry level.

**Note**: Functional and policy guidance on creating and maintaining the records classification structure will be provided to workgroups by the appropriate authority (e.g., Senior Records Officer).

Responsibility: Senior Records Officer

## *2.3 Folder Metadata*

Mandatory metadata elements are to be assigned to folders managed in EIM. The mandatory metadata elements for folders are:

- records classification structure codes;
- folder title;
- access restrictions; and
- recording medium (electronic, non-electronic, both).

Responsibility: Senior Records Officer/Administrator

## 2.4 User Profile

**Ministries will maintain a profile on each authorized EIM user. User profiles will include the following:**

**[Insert GoA Standard when completed. Lead: Innovation and Science, Office of the Corporate Chief Information Officer.]**

Responsibility: Administrator

## 2.5 Maintaining Audit Data

Audit data generated by or within EIM will be maintained as a record by the EIM Administrator.

Audit data will:

- record activities associated with electronic documents and their metadata such as save, modify, read and delete - this data is to be retained according to the appropriate records retention and disposition schedules;
- record activities at the operating system level - this data should be retained for 12 months;
- record activities at the system level such as backups and restores - this data should be retained for 12 months; and
- record activities associated with the check-out / check-in of paper files – this data is to be retained for the life of the paper file.

Responsibility: Administrator

Note: A records retention and disposition schedule for the above has not been established.

## 2.6 Information Access

Content items managed in the EIM repository will be, by default, shareable and accessible to any ministry employee.

The controller (author), a delegate or the workgroup EIM Administrator is responsible for ensuring items that must have restricted access are adequately protected (based on security classification). This may include limiting access to specific workgroups or specific users.

Responsibility: Controller

## 2.7 Search and Retrievals

Search and retrieval of documents and profiles within EIM will be, by default, performed by accessing the workgroup repository. Searches can be expanded by accessing metadata resident in other repositories. Access restrictions will be followed and, for confidential and restricted classification, the documents will not appear on the search results screen.

**Note**: Searching repositories outside the workgroup will normally be performed by exception; also, the ability to search for documents from other repositories may be limited by access restrictions.

Responsibility: Administrator

## 2.8 Modifying Draft Content Items

A draft of an electronic content item, (i.e. the most recent version), stored within EIM that is not declared an official record may be modified by the original author of the document (controller) or delegate. Other EIM users attempting to modify a draft document not authored by them will be required to save it as a new document.

Exception: When a draft electronic content item is authored collaboratively, i.e., by two or more people, the users granted co-authoring rights will be permitted to modify the content item, see " Collaborative Authoring."

Responsibility: Administrator

## 2.9 Deleting Content Items

An electronic content item and versions of content items managed within EIM that are transitory records can be deleted by the original author, their delegate, or the workgroup EIM Administrator. These content items will be flagged for deletion and retained within the system for a specified period of time before actual destruction. Content items that have been declared official records cannot be deleted as a transitory record. They must follow an approved records retention and disposition schedule.

Responsibility: Controller, Administrator

## 2.10 Remote Access to EIM

**Remote or mobile access to EIM functions and repositories will be performed through a secure link (e.g., Citrix). [Lead: Innovation and Science, Office of the Corporate Chief Information Officer]**

**Note**: Ministries should have established practices related to records downloaded to remote devices (e.g., hand-held PDAs).

Responsibility: Controller, Administrator

### 2.11 *Quality Control – Organization, Transmission, Use and Retrieval*

The Administrator or workgroup EIM Administrator will be responsible for performing quality control on all aspects associated with the organization, transmission, use and retrieval of records managed within EIM. This will include ensuring that the appropriate records classification codes and metadata are assigned to electronic documents and references to collections of documents.

Responsibility: Administrator

# 3.
# Storage and Protection

Appropriate practices for storage and protection will be applied to ensure the integrity of recorded information. This includes the continued readability of electronic information. Records that have been declared official records must be protected against loss and unauthorized access, use, alteration, destruction or alienation. Special measures will be taken for the security of confidential and restricted information, which will be reflected in record keeping procedures.

## *3.1 Storage of Electronic Content Items and Profiles*

To promote efficiencies and economies, electronic content items and profiles managed within EIM will be stored in various media and locations.

For example:

- on-line storage will be reserved for immediate (on-line) access to documents, associated metadata and other associated files, e.g. document indexes and audit logs, in active, functional use;
- near-line storage methods will be used for semi-active or inactive documents, i.e., that are no longer in constant use but may be required from time to time. These documents may be stored on near-line storage media such as optical disks which are kept on-site. The document metadata and document indexes and audit logs associated with inactive documents in near-line storage will be maintained on-line until the documents are officially disposed; and
- off-line storage will be used for dormant documents, i.e., documents that are no longer in constant use but may be required at some future time. These documents will be stored on off-line storage media usually in an off-site storage facility, see "Off-Site Storage." The document metadata and document indexes and audit logs associated with documents stored off-line will be maintained on-line until the documents are officially disposed.

**Note**: The criteria for storing and migrating documents to each medium and location will be dependent primarily on:

- access rates;
- records retention and disposition schedule including final disposition;
- security requirements;
- protection requirements; and
- the availability of storage space.

**Note**: Setting workgroup specific criteria for storing, migrating and backing up documents will be the responsibility of the workgroup EIM Administrator with guidance provided by the ministry. The workgroup EIM Administrator together with the ministry network administrator will be responsible for managing the storage and migration of documents to different media and locations.

Responsibility: Administrator

### 3.2 Storage of Metadata

Metadata associated with a content item or a collection of content items will remain on-line until the content items are officially disposed of, regardless of their storage medium or location. Metadata associated with a folder, will be retained permanently.

Responsibility Level: Administrator

### 3.3 Inherit Security Attributes of Records Classification Code

Electronic content items managed within EIM and non-electronic content items profiled in EIM are associated to a records classification code within the records classification structure will inherit the security attributes of the records classification code. The inherited security attributes will govern access to and protection of the content items.

Responsibility: Controller/Steward/Administrator

### 3.4 Access Restrictions

The controller (author) can establish access restrictions on content items managed in EIM. Access can be restricted to individuals or to groups.

Access restrictions can be set to:

- allow users the ability to view the metadata within a search results list but not be able to access the document or content item; or
- to prevent users from viewing metadata within the search results lists thus providing no indication that a particular document or content item exists; and
- to prevent users from viewing folder metadata within the search results lists thus providing no indication that a particular folder exists.

**Note**: One of the objectives of EIM is to ensure that information within the ministry is shareable and accessible. To this end, it is the responsibility of the workgroup EIM Administrator to monitor the degree and nature of access restrictions placed on content items and folders to ensure that such restrictions are not being misused.

Responsibility: Controller/Administrator

### 3.5 *Rights and Privileges*

To manage the integrity and reliability of documents and to ensure the EIM system operates at peak efficiency and effectiveness, rights and privileges will be established for all EIM users and administrators.

The controller (author) will have the ability to:

- store a content item within EIM;
- create new versions of a content item they have authored;
- modify a content item that has not been declared an official record and the associated metadata;
- declare a content item as official records, and
- delete transitory records, (see "Official Records within EIM").

The EIM Administrator will have full rights to manage the EIM system. In addition to the rights of a user, the EIM Administrator will have the ability to:

- add / remove / modify user accounts;
- add / remove / modify workgroup specific metadata fields;
- add to or modify the records classification structure, including retention periods (with the approval of the SRO);
- assign rights to an author's delegate; and
- access and maintain EIM administrative software components.

Responsibility: Controller/Administrator

### 3.6 *Inherit Vital Records Attributes of Records Classification Code*

Electronic content items managed within EIM are associated to a records classification code within the records classification structure and will inherit the Vital Records attributes of the records classification code.

**Note**: The inherited Vital Records attributes will govern what measures are taken to protect the document.

Responsibility: Administrator

### 3.7 Vital Records – Disaster Recovery

To make vital records and information systems operational in the event of a natural disaster or other destructive occurrence, special emergency operating sites will be maintained at secure facilities located off-site.

**Note**: The ministry is responsible to ensure that vital records are available according to government business continuity planning practices.

Responsibility: Administrator

### 3.8 Migrating Content Items to Upgraded Software

A record will remain in the format of the software version it was originally created, for the life of the record. If the record needs to be viewed and the originating software is no longer available the following options will be exercised:

- a generic software viewer will be used;
- the content item will be converted to a more recent software version or environment for viewing, note: if modifications are made to the document and the document, it will be saved in the new format; and
- if the content item is a final official record and it is modified, it must be saved as a new content item.

**Note**: It is the responsibility of the user and the workgroup EIM Administrator to ensure that content items remain, where possible, in the format of the original software version.

**Note**: Performing mass migrations of content items to new software versions and environments will not be undertaken, unless by not performing the migration the content items will be rendered unreadable.

**Note**: The practices outlined here are for the management of records in EIM within the ministry. Practices related to records to be transferred to the Provincial Archives will be added when the corporate digital preservation strategy is completed. [Lead: Government Services, Information Management and Community Development, Provincial Archives.]

Responsibility: Controller/Steward/Administrator

### 3.9 Transferring Access Rights to a Different User

The workgroup EIM Administrator may, at the direction of the workgroup manager, transfer access rights to content items and folders created by a departed member of the workgroup to another workgroup user(s).

Note: This action will depend on the security classification attached to content items and will permit the workgroup manager to change access restrictions to documents that were set by former members of the workgroup.

Responsibility: Administrator

### 3.10 Transferring Content Items to a Different Workgroup

Responsibility for managing electronic and non-electronic content (and associated metadata and audit logs) which support a continuing function must be assigned to the workgroup responsible for the function, whether or not they initially created or received the documents.

**Note**: The receiving workgroup assumes control over the documents, metadata and audit logs, including the right to assign new life cycle attributes, e.g., retention and disposition schedules; see "Retention and Disposition."

Responsibility: Ministry Steward/Administrator

### 3.11 Quality Control: Storage and Protection

The workgroup EIM Administrator will be responsible for performing quality control on all aspects associated with the storage and protection of records managed within EIM. This will include ensuring that:

- content items are transferred to appropriate storage media and locations according to established criteria and procedures;
- content items remain accessible and shareable, where appropriate, to all ministry employees; and
- appropriate measures are taken to protect Vital Records.

Responsibility: Administrator

# 4.
# Retention and Disposition

Retention and disposition is an important component of the life cycle management of records and information. It is governed by formal processes and practices to support compliance with the Records Management Regulation.

Records retention and disposition schedules developed by individual ministries and approved by the Alberta Records Management Committee (ARMC) will govern the retention and disposition of all records. These schedules set out designated retention periods to ensure that records are maintained and protected for as long as they are needed, (for their operational, fiscal and/or legal value and in accordance with privacy requirements). The schedules also identify records deemed to have archival value and, as such, are subject to transfer to the Provincial Archives at the end of their retention period. Related procedures and directives for scheduling and disposition will be maintained.

## *4.1 Retention – Assigning Retention Periods*

**Retention periods are established in records retention and disposition schedules approved by the Alberta Records Management Committee (ARMC)**
[Lead: Government Services, Information Management Branch]

All records managed within EIM will be assigned a retention period. Retention periods will be assigned to content items through their association to records classification codes within the records classification structure.

**Note**: It is the responsibility of the program managers to consult with the Senior Records Officer (SRO) to identify the retention periods for documents of the workgroup. It is the responsibility of the ministry SRO to submit records retention and disposition schedules to the ARMC for approval. It is the responsibility of the SRO, along with the Administrator/EIM Administrator to ensure that retention periods exist within the workgroup records classification structure. Guidance on developing retention periods can be obtained from the Senior Records Officer.

Responsibility: SRO/Administrator

## *4.2 Inherit Retention Period Assigned to Records Classification Code*

Content items managed within EIM are associated to a records classification code within the records classification structure and will inherit the retention period assigned to the classification code.

Responsibility: Administrator

### 4.3 Retention Period – Extend or Suspend

The EIM Administrator, acting on behalf of the Ministry or workgroup manager, and under the direction of the SRO, will have the right to extend or suspend (freeze) the retention period of an individual content item or collection of content items.

**Note**: This measure will be used on an exception basis pursuant to a court order, an outstanding request made under provisions of the *Freedom of Information and Protection of Privacy Act* or to a related investigation, or due to other conditions that alter the normal operational, legal or fiscal value of the document(s).

Responsibility: Administrator/SRO

### 4.4 Disposition – Records Retention and Disposition Schedule

The disposition of all records managed within EIM will be conducted through the application of a Records Retention and Disposition Schedule. Disposition specifications will be assigned to documents through their association to records classification codes within a records classification structure.

**Note**: The SRO is responsible for obtaining authority for the disposition of records through the ministry and, once obtained, for assigning disposition specifications to records classification codes within the workgroup records classification structure, and for conducting disposition action upon the completion of the retention periods in accordance to the records retention and disposition schedules.

Responsibility: Administrator/SRO

### 4.5 Disposition – Metadata

Content item metadata will be disposed of in the same manner as the associated content item, with the exception of the certificate of final disposition, which will be kept permanently.

Responsibility: Administrator

### 4.6 Disposition – Folder Metadata

Folder metadata will be kept permanently.

**Note**: A copy of folder metadata for content items transferred to the Provincial Archives will be also transferred with the associated content items.

Responsibility: Administrator

### 4.7 Disposition – Workgroup Manager Approval

Approval for the disposition of any records managed by EIM (electronic and non-electronic) must be obtained from the workgroup manager prior to undertaking the actual disposition.

Responsibility: Administrator/SRO

### 4.8 Retention and Disposition – Records Classification Structure Audit Trail

The workgroup records classification structure, with data and audit records that document final disposition actions, will be maintained indefinitely. Data on the activity associated with a paper file volume, e.g. check-out / in, should be maintained for the life of the volume.

**Note**: It is the responsibility of the workgroup EIM Administrator to maintain and preserve copies of the records classification structure and all associated records that document disposition action.

Responsibility: SRO/Records Management

### 4.9 Final Disposition

The authorized final disposition (i.e. destruction or transfer to the Provincial Archives) of EIM content items will include:

*For Destruction*

- the complete disposition of the electronic content items, attachments, and metadata from all storage media, e.g., on-line, near-line discs, tapes;
- the complete disposition of all non-electronic content items, including folders, (excluding folder metadata).

**Note**: The disposition action will be such that the content item (including attachments) and associated data files cannot be re-constructed without extraordinary means.

*For Transfer to Provincial Archives*

To be developed in EIM Phase 2 as part of the Corporate Digital Preservation Strategy.

Responsibility: Administrator/SRO

### 4.10 Quality Control: Retention and Disposition

The workgroup EIM Administrator will be responsible for performing quality control on all aspects associated with the disposition of records managed within EIM. This will include ensuring that:

- retention and disposition conditions approved by the Alberta Records Management Committee (ARMC) are assigned to all electronic and non-electronic records;
- suspensions or "freezes" of retention periods are only invoked according to defined criteria and are lifted when appropriate;
- inactive records are transferred in accordance with approved records retention and disposition schedules and with the approval of the workgroup manager;
- all duplicates of records have been disposed of or transferred;
- the approved destruction of records is complete; and
- the transfer of archival electronic records to the Provincial Archives is complete.

Responsibility: Administrator

# Glossary

| | |
|---|---|
| Content Item | Any information content.<br><br>Examples of "content items" include:<br>▪ office documents, such as reports, letters, presentations, spreadsheets, e-mail messages and attachments; notes and discussions threads;<br>▪ graphical objects and images, often combined with or embedded in documents;<br>▪ multimedia items, e.g. sound and video; and<br>▪ web content (both publications and other forms of content). |
| Controller | The author or creator of information content. |
| EIM Administrator | The systems administrator managing EIM within the ministry. Where needed, administrators may be appointed for a workgroup. |
| Steward | Those individuals in the organization that handle, process, collect or update information content for controllers. |
| User | Any individual who uses information content managed within EIM. Users may be decision-makers, team members, and others who are not involved in the creation of information content. |